

# Construction of $\mathbb{Z}_4$ -linear Reed-Muller codes\*

J. Pujol, J. Rifà, F. I. Solov'eva<sup>†</sup>

## Abstract

New quaternary Plotkin constructions are given and are used to obtain new families of quaternary codes. The parameters of the obtained codes, such as the length, the dimension and the minimum distance are studied. Using these constructions new families of quaternary Reed-Muller codes are built with the peculiarity that after using the Gray map the obtained  $\mathbb{Z}_4$ -linear codes have the same parameters and fundamental properties as the codes in the usual binary linear Reed-Muller family. To make more evident the duality relationships in the constructed families the concept of Kronecker inner product is introduced.

## 1 Introduction

In [13] Nechaev introduced the concept of  $\mathbb{Z}_4$ -linearity of binary codes and later, in [7], Hammons, Kumar, Calderbank, Sloane and Solé showed that several families of binary codes are  $\mathbb{Z}_4$ -linear. In [7] it is proved that the binary linear Reed-Muller code  $RM(r, m)$  is  $\mathbb{Z}_4$ -linear for  $r = 0, 1, 2, m-1, m$  and is not  $\mathbb{Z}_4$ -linear for  $r = m-2$  ( $m \geq 5$ ). In a subsequent work, Hou, Lahtonen and Koponen [8], proved that  $RM(r, m)$  is not  $\mathbb{Z}_4$ -linear for  $3 \leq r \leq m-2$ .

In [7] it is introduced a construction of codes, called  $QRM(r, m)$ , based on  $\mathbb{Z}_4$ -linear codes, such that after doing modulo two we obtain the usual binary linear Reed-Muller ( $RM$ ) codes. In [2, 3] such family of codes is studied and their parameters are computed as well as the dimension of the kernel and rank. In [16] a kind of Plotkin construction was used to build a family of additive Reed-Muller codes and also in [19] it was used a Plotkin construction to obtain a sequence of quaternary linear Reed-Muller like codes. In both last quoted constructions, the images of the obtained codes under the Gray map are binary codes with the same parameters as the binary linear  $RM$  codes. Moreover, on the other hand, in [5, 9, 10, 14] were classified all the non-equivalent  $\mathbb{Z}_2\mathbb{Z}_4$ -linear extended 1-perfect codes and their duals, the  $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes. It

---

\*This work has been partially supported by the Spanish MEC and the European FEDER Grant MTM2006-03250. Part of the material in Section III of this paper was presented at the 17th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes (AAECC), Bangalore, India, December 2007.

<sup>†</sup>J. Pujol and J. Rifà are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. F. I. Solov'eva is with the Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia.

is a natural question to ask for the existence of families of quaternary linear codes such that, after the Gray map, the corresponding  $\mathbb{Z}_4$ -linear codes have the same parameters as the well known family of binary linear  $RM$  codes. In these new families, like in the usual  $RM(r, m)$  family, the code with  $(r, m) = (1, m)$  should be a Hadamard code and the code with  $(r, m) = (m - 2, m)$  should be an extended 1-perfect code.

It is well known that an easy way to build the binary  $RM$  family of codes is by using the Plotkin construction [12]. So, it seems a good matter of study to try to generalize the Plotkin construction to the quaternary linear codes and try to obtain new families of codes which contain the above mentioned  $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes and  $\mathbb{Z}_2\mathbb{Z}_4$ -linear extended 1-perfect codes and fulfill the same properties from a parameters point of view (length, dimension, minimum distance, inclusion and duality relationship) than the binary  $RM$  family.

In this paper we begin by studying the  $\mathbb{Z}_4$ -linear case and we organize it in the following way. In Section 2 we introduce the concept of quaternary code and give some constructions that could be seen as quaternary generalizations of the well known binary Plotkin construction. In Section 3, we construct several families of  $\mathbb{Z}_4$ -linear Reed-Muller codes and prove that they have similar parameters as the classical binary  $RM$  codes but they are not linear. In Section 4, we discuss the concept of duality for the constructed  $\mathbb{Z}_4$ -linear Reed-Muller codes and, finally, in Section 5 we give some conclusions and further research in the topic.

## 2 Constructions of quaternary codes

### 2.1 Quaternary codes

Let  $\mathbb{Z}_2$  and  $\mathbb{Z}_4$  be the ring of integers modulo two and modulo four, respectively. Let  $\mathbb{Z}_2^n$  be the set of all binary vectors of length  $n$  and  $\mathbb{Z}_4^N$  be the set of all quaternary vectors of length  $N$ . Any non-empty subset  $C$  of  $\mathbb{Z}_2^n$  is a binary code and a subgroup of  $\mathbb{Z}_2^n$  is called a *binary linear code*. Equivalently, any non-empty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*. In general, any non-empty subgroup  $\mathcal{C}$  of  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$  is an *additive code*.

The Hamming weight  $w_H(\mathbf{u})$  of a vector in  $\mathbb{Z}_2^n$  is the number of its nonzero coordinates. The Hamming distance  $d(\mathbf{u}, \mathbf{v})$  between two vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$  is  $d(\mathbf{u}, \mathbf{v}) = w_H(\mathbf{u} - \mathbf{v})$ . For quaternary codes it is more appropriate to use the Lee metric [11]. In  $\mathbb{Z}_2$  the Lee weight coincides with the Hamming weight, but in  $\mathbb{Z}_4$  the Lee weight of their elements is  $w_L(0) = 0, w_L(1) = w_L(3) = 1$ , and  $w_L(2) = 2$ . The Lee weight  $w_L(\mathbf{u})$  of a vector in  $\mathbb{Z}_4^N$  is the addition of the Lee weight of all the coordinates. The Lee distance  $d_L(\mathbf{u}, \mathbf{v})$  between two vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^N$  is  $d_L(\mathbf{u}, \mathbf{v}) = w_L(\mathbf{u} - \mathbf{v})$ .

Let  $\mathcal{C}$  be an *additive code*, so a subgroup of  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$  and let  $C = \Phi(\mathcal{C})$ , where  $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$ ,  $n = \alpha + 2\beta$ , is given by  $\Phi(\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \phi(\mathbf{v}))$  for any  $\mathbf{u}$  from  $\mathbb{Z}_2^\alpha$  and any  $\mathbf{v}$  from  $\mathbb{Z}_4^\beta$ , where  $\phi : \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^{2\beta}$  is the usual Gray map, so  $\phi(v_1, \dots, v_\beta) = (\varphi(v_1), \dots, \varphi(v_\beta))$ , and  $\varphi(0) = (0, 0), \varphi(1) = (0, 1), \varphi(2) =$

$(1, 1)$ ,  $\varphi(3) = (1, 0)$ . We will use the symbols  $\mathbf{0}$ ,  $\mathbf{1}$  and  $\mathbf{2}$  for the all zeroes, the all ones and the all twos vectors, respectively (by the context it will be always clear we speak about the binary vectors  $\mathbf{0}$ ,  $\mathbf{1}$  or quaternary, it will also be clear the length of the vectors).

Hamming and Lee weights, as well as Hamming and Lee distances, can be generalized, in a natural way, to vectors in  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$  by adding the corresponding weights (or distances) of the  $\mathbb{Z}_2^\alpha$  part and the  $\mathbb{Z}_4^\beta$  part.

Since  $\mathcal{C}$  is a subgroup of  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ , it is also isomorphic to an abelian structure like  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ . Therefore, we have that  $|\mathcal{C}| = 2^{\gamma+2\delta}$  and the number of order two codewords in  $\mathcal{C}$  is  $2^{\gamma+\delta}$ . We call such code  $\mathcal{C}$  an *additive code of type*  $(\alpha, \beta; \gamma, \delta)$  and the binary image  $C = \Phi(\mathcal{C})$  a  $\mathbb{Z}_2\mathbb{Z}_4$ -linear code of type  $(\alpha, \beta; \gamma, \delta)$ . In the specific case  $\alpha = 0$  we see that  $\mathcal{C}$  is a quaternary linear code and its binary image is called a  $\mathbb{Z}_4$ -linear code. Note that the binary length of the binary code  $C = \Phi(\mathcal{C})$  is  $n = \alpha + 2\beta$ .

The minimum Hamming distance  $d$  of a  $\mathbb{Z}_2\mathbb{Z}_4$ -linear code  $C$  is the minimum value of  $d(\mathbf{u}, \mathbf{v})$ , where  $\mathbf{u}, \mathbf{v} \in C$  and  $\mathbf{u} \neq \mathbf{v}$ . Notice that the Hamming distance of a  $\mathbb{Z}_2\mathbb{Z}_4$ -linear code  $C$  coincides with the Lee distance defined in the additive code  $\mathcal{C} = \Phi^{-1}(C)$ . From now on, when we work with distances it must be understood that we deal with Hamming distances in the case of binary codes or Lee distances in the case of additive codes.

Although  $\mathcal{C}$  could not have a basis, it is appropriate to define a generator matrix for  $\mathcal{C}$  as

$$\mathcal{G} = \left( \begin{array}{c|c} B_2 & Q_2 \\ \hline B_1 & Q_1 \end{array} \right),$$

where  $B_2$  is a  $\gamma \times \alpha$  matrix;  $Q_2$  is a  $\gamma \times \beta$  matrix;  $B_1$  is a  $\delta \times \alpha$  matrix and  $Q_1$  is a  $\delta \times \beta$  matrix. Matrices  $B_1, B_2$  are binary and  $Q_1, Q_2$  are quaternary, but the entries in  $Q_2$  are only zeroes or twos.

Two additive codes  $\mathcal{C}_1$  and  $\mathcal{C}_2$  both of the same length are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and multiplying by  $-1$  of certain coordinates. Additive codes which differ only by a permutation of coordinates are said to be *permutation equivalent*.

For  $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes is usual to use the following definition of inner product in  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$  that we will call the *standard inner product* [18, 4]:

$$\langle \mathbf{u}, \mathbf{v} \rangle = 2 \left( \sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \in \mathbb{Z}_4, \quad (1)$$

where  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ . We can also write the standard inner product as

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u} \cdot J_N \cdot \mathbf{v}^t,$$

where  $J_N = \left( \begin{array}{c|c} 2I_\alpha & \mathbf{0} \\ \hline \mathbf{0} & I_\beta \end{array} \right)$ ,  $N = \alpha + \beta$ , is a diagonal matrix over  $\mathbb{Z}_4$ . Note that when  $\alpha = 0$  the inner product is the usual one for vectors over  $\mathbb{Z}_4$  and when  $\beta = 0$  it is twice the usual one for vectors over  $\mathbb{Z}_2$ .

For  $\alpha = 0$  and  $N = \beta = 2^i$ ,  $i = 1, 2, 3, \dots$ , we can define the inner product in an alternative way. Let  $K_2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$  be a matrix over  $\mathbb{Z}_4$  and define  $K_N = \bigotimes_{j=1}^{\log_2(N)} K_2$  where  $\bigotimes$  denotes the Kronecker product of matrices. We call the *Kronecker inner product* the following:

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = \mathbf{u} \cdot K_N \cdot \mathbf{v}^t. \quad (2)$$

The *additive dual code* of  $\mathcal{C}$ , denoted by  $\mathcal{C}^\perp$ , is defined in the standard way as

$$\mathcal{C}^\perp = \{ \mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \langle \mathbf{u}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{v} \in \mathcal{C} \}$$

or, using the Kronecker inner product

$$\mathcal{C}^\perp = \{ \mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0 \text{ for all } \mathbf{v} \in \mathcal{C} \}.$$

The definition and notations will be the same for the  $\mathbb{Z}_4$ -duality obtained by using the standard inner product or the Kronecker inner product and the difference will be clear from the context.

Note that  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = \mathbf{u} \cdot K_N \cdot \mathbf{v}^t = \langle \mathbf{u}, \mathbf{v} \cdot K_N \rangle$ . Hence, both additive dual codes by using the standard inner product or the Kronecker inner product, respectively, are monomially equivalent and so they have the same weight distribution. For both inner products, the additive dual code  $\mathcal{C}^\perp$  is also an additive code, that is a subgroup of  $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ . Its weight enumerator polynomial is related to the weight enumerator polynomial of  $\mathcal{C}$  by the MacWilliams identity [6]. The corresponding binary code  $\Phi(\mathcal{C}^\perp)$  is denoted by  $C_\perp$  and called the  *$\mathbb{Z}_2\mathbb{Z}_4$ -dual code* of  $\mathcal{C}$ . In the case  $\alpha = 0$ , the code  $\mathcal{C}^\perp$  is also called the *quaternary dual code* of  $\mathcal{C}$  and  $C_\perp$  the  *$\mathbb{Z}_4$ -dual code* of  $\mathcal{C}$ . Notice that  $\mathcal{C}$  and  $C_\perp$  are not dual in the binary linear sense but the weight enumerator polynomial of  $C_\perp$  is the McWilliams transform of the weight enumerator polynomial of  $\mathcal{C}$ . Given an additive code  $\mathcal{C}$  of type  $(\alpha, \beta, \gamma, \delta)$  it is known the type of the additive dual code ([4] for additive codes with  $\alpha \neq 0$  and [7] for additive codes with  $\alpha = 0$ ).

In the present paper, as we will see later, the duality concept using the Kronecker inner product will make more visible the property that if a code  $\mathcal{C}$  belongs to a family of Reed-Muller codes then its dual code belongs to the same family.

From now on, we focus our attention specifically to additive codes with  $\alpha = 0$ , so quaternary linear codes such that after the Gray map they give rise to  $\mathbb{Z}_4$ -linear codes. Given a quaternary linear code of type  $(0, \beta; \gamma, \delta)$ , we will write  $(N; \gamma, \delta)$  to say that  $\alpha = 0$  and  $\beta = N$ .

## 2.2 The Plotkin construction

In this section, we show that the well-known binary Plotkin construction can be generalized to quaternary linear codes.

Let  $\mathcal{A}$  and  $\mathcal{B}$  be two quaternary linear codes of types  $(N; \gamma_{\mathcal{A}}, \delta_{\mathcal{A}})$  and  $(N; \gamma_{\mathcal{B}}, \delta_{\mathcal{B}})$  and minimum distances  $d_{\mathcal{A}}$ ,  $d_{\mathcal{B}}$ , respectively. Given  $\mathbf{u} \in \mathbb{Z}_4^N$  define  $\text{supp}(\mathbf{u}) \subset \{1, \dots, N\}$  as the set of nonzero coordinates of vector  $\mathbf{u}$ .

**Definition 1 (Plotkin Construction)** *Given two quaternary linear codes  $\mathcal{A}$  and  $\mathcal{B}$ , we define a quaternary linear code as*

$$\mathcal{PC}(\mathcal{A}, \mathcal{B}) = \{(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2) : \mathbf{u}_1 \in \mathcal{A}, \mathbf{u}_2 \in \mathcal{B}\}.$$

It is easy to see that if  $\mathcal{G}_{\mathcal{A}}$  and  $\mathcal{G}_{\mathcal{B}}$  are generator matrices of  $\mathcal{A}$  and  $\mathcal{B}$ , respectively, then the matrix

$$\mathcal{G}_{PC} = \begin{pmatrix} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}_{\mathcal{B}} \end{pmatrix}$$

is a generator matrix of the code  $\mathcal{PC}(\mathcal{A}, \mathcal{B})$ .

**Proposition 2** *The quaternary linear code  $\mathcal{PC}(\mathcal{A}, \mathcal{B})$  defined using the Plotkin construction is of type  $(2N; \gamma, \delta)$ , where  $\gamma = \gamma_{\mathcal{A}} + \gamma_{\mathcal{B}}$  and  $\delta = \delta_{\mathcal{A}} + \delta_{\mathcal{B}}$ ; the binary length is  $n = 4N$ ; the size is  $2^{\gamma+2\delta}$  and the minimum distance is  $d = \min\{2d_{\mathcal{A}}, d_{\mathcal{B}}\}$ .*

*Proof:* The type, the binary length and the size of  $\mathcal{PC}(\mathcal{A}, \mathcal{B})$  can be easily computed from the definition of the code. The minimum distance can be established as in the binary case [12] but, by completeness, we include the proof. Let us consider any vector  $\mathbf{u} \in \mathcal{PC}(\mathcal{A}, \mathcal{B})$  such that  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2)$ , where  $\mathbf{u}_1 \in \mathcal{A}$  and  $\mathbf{u}_2 \in \mathcal{B}$ . Since  $\mathcal{PC}(\mathcal{A}, \mathcal{B})$  is a quaternary linear code, it is enough to prove that the weight  $w_L(\mathbf{u})$  is not less than  $d$ .

If  $\mathbf{u}_2 = \mathbf{0}$ , then  $w_L(\mathbf{u}) = 2w_L(\mathbf{u}_1) \geq 2d_{\mathcal{A}}$ .

If  $\mathbf{u}_2 \neq \mathbf{0}$ , by using the triangle inequality we immediately obtain

$$w_L(\mathbf{u}) = w_L(\mathbf{u}_1) + w_L(\mathbf{u}_1 + \mathbf{u}_2) \geq w_L(\mathbf{u}_2) \geq d_{\mathcal{B}}.$$

Hence  $d \geq \min\{2d_{\mathcal{A}}, d_{\mathcal{B}}\}$ . The equality holds because taking the specific vectors  $\mathbf{u}_1 \in \mathcal{A}$  with minimum weight  $d_{\mathcal{A}}$  and  $\mathbf{u}_2 \in \mathcal{B}$  with minimum weight  $d_{\mathcal{B}}$  we obtain  $w_L(\mathbf{u}_1 | \mathbf{u}_1) = 2d_{\mathcal{A}}$  and  $w_L(\mathbf{0} | \mathbf{v}_2) = d_{\mathcal{B}}$ .  $\square$

### 2.3 The quaternary Plotkin construction

A useful generalization of the above construction to obtain quaternary linear codes is the following construction, called the *quaternary Plotkin construction*. Such construction was used, for example, in [10] for the classification of all  $\mathbb{Z}_4$ -linear Hadamard codes.

**Definition 3 (Quaternary Plotkin Construction)** *Given two quaternary linear codes  $\mathcal{A}$  and  $\mathcal{B}$ , we define the quaternary linear code*

$$\mathcal{QP}(\mathcal{A}, \mathcal{B}) = \{(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2 | \mathbf{u}_1 + 2\mathbf{u}_2 | \mathbf{u}_1 + 3\mathbf{u}_2) : \mathbf{u}_1 \in \mathcal{A}, \mathbf{u}_2 \in \mathcal{B}\}.$$

It is easy to see that if  $\mathcal{G}_{\mathcal{A}}$  and  $\mathcal{G}_{\mathcal{B}}$  are generator matrices of  $\mathcal{A}$  and  $\mathcal{B}$ , then the matrix

$$\mathcal{G}_{QP} = \begin{pmatrix} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}_{\mathcal{B}} & 2\mathcal{G}_{\mathcal{B}} & 3\mathcal{G}_{\mathcal{B}} \end{pmatrix}$$

is a generator matrix of the code  $\mathcal{QP}(\mathcal{A}, \mathcal{B})$ .

**Proposition 4** *The quaternary linear code  $\mathcal{QP}(\mathcal{A}, \mathcal{B})$  given in Definition 3 is of type  $(4N; \gamma, \delta)$ , where  $\gamma = \gamma_{\mathcal{A}} + \gamma_{\mathcal{B}}$  and  $\delta = \delta_{\mathcal{A}} + \delta_{\mathcal{B}}$ ; the binary length is  $n = 8N$ ; the size is  $2^{\gamma+2\delta}$  and the minimum distance is  $d \geq \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}\}$ .*

*Proof:* The type, the binary length and the size of  $\mathcal{QP}(\mathcal{A}, \mathcal{B})$  can be easily computed from the definition of the code. To check the minimum distance of  $\mathcal{QP}(\mathcal{A}, \mathcal{B})$  let us consider any vector  $\mathbf{u} \in \mathcal{QP}(\mathcal{A}, \mathcal{B})$ . Vector  $\mathbf{u}$  can be represented by  $\mathbf{u} = (\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1) + (\mathbf{0}|\mathbf{u}_2|2\mathbf{u}_2|3\mathbf{u}_2)$ , where  $\mathbf{u}_1 \in \mathcal{A}$  and  $\mathbf{u}_2 \in \mathcal{B}$ . Since  $\mathcal{QP}(\mathcal{A}, \mathcal{B})$  is a quaternary linear code it is enough to show that the weight of  $\mathbf{u}$  is at least  $d$ .

If  $\mathbf{u}_2 = \mathbf{0}$ , then  $w_L(\mathbf{u}) = 4w_L(\mathbf{u}_1) \geq 4d_{\mathcal{A}}$ . The equality holds taking a vector  $\mathbf{u}_1 \in \mathcal{A}$  of minimum weight.

For  $\mathbf{u}_2 \neq \mathbf{0}$  we have

$$\begin{aligned} w_L(\mathbf{u}) &= w_L(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2|\mathbf{u}_1 + 2\mathbf{u}_2|\mathbf{u}_1 + 3\mathbf{u}_2) \\ &= (w_L(\mathbf{u}_1) + w_L(\mathbf{u}_1 + \mathbf{u}_2)) + (w_L(\mathbf{u}_1 + 2\mathbf{u}_2) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_2)) \\ &\geq w_L(\mathbf{u}_2) + w_L(\mathbf{u}_2) \text{ (by using the triangle inequality)} \\ &\geq 2d_{\mathcal{B}}. \end{aligned}$$

□

The Plotkin and the quaternary Plotkin constructions can be combined in a *double Plotkin construction*. Let  $\mathcal{A}$ ,  $\mathcal{B}$ ,  $\mathcal{C}$  and  $\mathcal{D}$  be four quaternary linear codes of types  $(N; \gamma_{\mathcal{A}}, \delta_{\mathcal{A}})$ ,  $(N; \gamma_{\mathcal{B}}, \delta_{\mathcal{B}})$ ,  $(N; \gamma_{\mathcal{C}}, \delta_{\mathcal{C}})$ , and  $(N; \gamma_{\mathcal{D}}, \delta_{\mathcal{D}})$  and minimum distances  $d_{\mathcal{A}}$ ,  $d_{\mathcal{B}}$ ,  $d_{\mathcal{C}}$ ,  $d_{\mathcal{D}}$ , respectively.

**Definition 5 (Double Plotkin Construction)** *Given  $\mathcal{A}$ ,  $\mathcal{B}$ ,  $\mathcal{C}$  and  $\mathcal{D}$  four quaternary linear codes, we define the quaternary linear code*

$$\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}) = \{(\mathbf{u}_1|\mathbf{u}_1+\mathbf{u}_2|\mathbf{u}_1+2\mathbf{u}_2+\mathbf{u}_3|\mathbf{u}_1+3\mathbf{u}_2+\mathbf{u}_3+\mathbf{u}_4) : \mathbf{u}_1 \in \mathcal{A}, \mathbf{u}_2 \in \mathcal{B}, \mathbf{u}_3 \in \mathcal{C}, \mathbf{u}_4 \in \mathcal{D}\}.$$

It is easy to see that if  $\mathcal{G}_{\mathcal{A}}$ ,  $\mathcal{G}_{\mathcal{B}}$ ,  $\mathcal{G}_{\mathcal{C}}$  and  $\mathcal{G}_{\mathcal{D}}$  are generator matrices of  $\mathcal{A}$ ,  $\mathcal{B}$ ,  $\mathcal{C}$  and  $\mathcal{D}$ , then the matrix

$$\mathcal{G}_{DP} = \begin{pmatrix} \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} & \mathcal{G}_{\mathcal{A}} \\ 0 & \mathcal{G}_{\mathcal{B}} & 2\mathcal{G}_{\mathcal{B}} & 3\mathcal{G}_{\mathcal{B}} \\ 0 & 0 & \mathcal{G}_{\mathcal{C}} & \mathcal{G}_{\mathcal{C}} \\ 0 & 0 & 0 & \mathcal{G}_{\mathcal{D}} \end{pmatrix}$$

is a generator matrix of the code  $\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$ .

**Proposition 6** *The quaternary linear code  $\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  given in Definition 5 is of type  $(4N; \gamma, \delta)$ , where  $\gamma = \gamma_{\mathcal{A}} + \gamma_{\mathcal{B}} + \gamma_{\mathcal{C}} + \gamma_{\mathcal{D}}$  and  $\delta = \delta_{\mathcal{A}} + \delta_{\mathcal{B}} + \delta_{\mathcal{C}} + \delta_{\mathcal{D}}$ ; the binary length is  $n = 8N$ ; the size is  $2^{\gamma+2\delta}$  and the minimum distance is  $d \geq \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, 2d_{\mathcal{C}}, d_{\mathcal{D}}\}$ .*

*Proof:* The type, the binary length and the size of the code  $\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  can be easily computed from the definition.

To check the minimum distance of the code  $\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  let us consider any vector  $\mathbf{u}$  from this code. It can be represented as  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1) + (\mathbf{0} | \mathbf{u}_2 | 2\mathbf{u}_2 | 3\mathbf{u}_2) + (\mathbf{0} | \mathbf{0} | \mathbf{u}_3 | \mathbf{u}_3) + (\mathbf{0} | \mathbf{0} | \mathbf{0} | \mathbf{u}_4)$ , where  $\mathbf{u}_1 \in \mathcal{A}$ ,  $\mathbf{u}_2 \in \mathcal{B}$ ,  $\mathbf{u}_3 \in \mathcal{C}$  and  $\mathbf{u}_4 \in \mathcal{D}$ . Since  $\mathcal{DP}(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D})$  is a quaternary linear code it is enough to show that the weight of  $\mathbf{u}$  is, at least,  $d$ .

If  $\mathbf{u}_2 = \mathbf{0}$  then we can write  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1) + (\mathbf{0} | \mathbf{0} | \mathbf{u}_3 | \mathbf{u}_3 + \mathbf{u}_4)$  so that  $\mathbf{u} \in \mathcal{PC}((\mathcal{A} | \mathcal{A}), \mathcal{PC}(\mathcal{C}, \mathcal{D}))$ , where  $(\mathcal{A} | \mathcal{A})$  is the code generated by  $(\mathcal{G}_A | \mathcal{G}_A)$ . Using Proposition 2 we obtain

$$w_L(\mathbf{u}) = \min\{2d_{(\mathcal{A} | \mathcal{A})}, d_{\mathcal{P}(\mathcal{C}, \mathcal{D})}\} = \min\{4d_A, \min\{2d_C, d_D\}\} = \min\{4d_A, 2d_C, d_D\}.$$

If  $\mathbf{u}_2 \neq \mathbf{0}$  then we distinguish two cases. If  $\mathbf{u}_4 = \mathbf{0}$  then  $w_L(\mathbf{u}) = w_L(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3 | \mathbf{u}_1 + 3\mathbf{u}_2 + \mathbf{u}_3) \geq w_L(\mathbf{u}_2) + w_L(\mathbf{u}_2) \geq 2d_B$  using twice the triangle inequality.

If  $\mathbf{u}_4 \neq \mathbf{0}$  then  $w_L(\mathbf{u}) = w_L(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3 | \mathbf{u}_1 + 3\mathbf{u}_2 + \mathbf{u}_3 + \mathbf{u}_4) \geq w_L(\mathbf{u}_2) + w_L(\mathbf{u}_2 + \mathbf{u}_4) \geq w_L(\mathbf{u}_4) \geq d_D$ .  $\square$

Note that in case  $\mathcal{B} = \mathcal{C}$  the bound is tight because  $d_B = d_C$  and the minimum distance  $d = \min\{4d_A, 2d_C, d_D\}$  can be obtained taking specific vectors from  $\mathcal{A}$ ,  $\mathcal{C}$  or  $\mathcal{D}$ .

## 2.4 The BQ-Plotkin construction

We slightly change the construction given in Definition 5 in order to obtain a tight bound for the minimum distance. We call this new construction the *BQ-Plotkin construction*.

Let  $\mathcal{A}$ ,  $\mathcal{B}$  and  $\mathcal{C}$  be three quaternary linear codes of types  $(N; \gamma_A, \delta_A)$ ,  $(N; \gamma_B, \delta_B)$ ,  $(N; \gamma_C, \delta_C)$ , with minimum distances  $d_A$ ,  $d_B$  and  $d_C$ , respectively.

**Definition 7 (BQ-Plotkin Construction)** Let  $\mathcal{G}_A$ ,  $\mathcal{G}_B$  and  $\mathcal{G}_C$  be generator matrices of the quaternary linear codes  $\mathcal{A}$ ,  $\mathcal{B}$  and  $\mathcal{C}$ , respectively. We define a new code  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  as the quaternary linear code generated by

$$\mathcal{G}_{BQ} = \begin{pmatrix} \mathcal{G}_A & \mathcal{G}_A & \mathcal{G}_A & \mathcal{G}_A \\ 0 & \mathcal{G}'_B & 2\mathcal{G}'_B & 3\mathcal{G}'_B \\ 0 & 0 & \hat{\mathcal{G}}_B & \hat{\mathcal{G}}_B \\ 0 & 0 & 0 & \mathcal{G}_C \end{pmatrix},$$

where  $\mathcal{G}'_B$  is the matrix obtained from  $\mathcal{G}_B$  after switching twos by ones in their  $\gamma_B$  rows of order two and  $\hat{\mathcal{G}}_B$  is the matrix obtained from  $\mathcal{G}_B$  after removing their  $\gamma_B$  rows of order two.

**Proposition 8** The quaternary linear code  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  is of type  $(4N; \gamma, \delta)$ , where  $\gamma = \gamma_A + \gamma_C$  and  $\delta = \delta_A + \gamma_B + 2\delta_B + \delta_C$ ; the binary length is  $n = 8N$ ; the size is  $2^{\gamma+2\delta}$  and the minimum distance  $d = \min\{4d_A, 2d_B, d_C\}$ .

*Proof:* The type, the length and the size of  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  can be easily computed from the definition of the code.

To check the minimum distance of  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  let us consider any vector  $\mathbf{u} = (\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1) + (\mathbf{0}|\mathbf{u}_2|2\mathbf{u}_2|3\mathbf{u}_2) + (\mathbf{0}|\mathbf{0}|\mathbf{u}_3|\mathbf{u}_3) + (\mathbf{0}|\mathbf{0}|\mathbf{0}|\mathbf{u}_4) \in \mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$ , where  $\mathbf{u}_1 \in \mathcal{A}$ ;  $\mathbf{u}_2 \in \mathcal{B}'$ ;  $\mathbf{u}_3 \in \hat{\mathcal{B}}$  and  $\mathbf{u}_4 \in \mathcal{C}$ . Codes  $\mathcal{B}'$  and  $\hat{\mathcal{B}}$  are the quaternary linear codes generated by  $\mathcal{G}'_{\mathcal{B}}$  and  $\hat{\mathcal{G}}_{\mathcal{B}}$ , respectively. Since  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  is a quaternary linear code it is enough to show that the weight of  $\mathbf{u}$  is at least  $d$ .

If  $\mathbf{u}_2 = \mathbf{0}$  then by using the same arguments as in Proposition 6 we have  $w_L(\mathbf{u}) \geq \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, d_{\mathcal{C}}\}$  because  $d_{\hat{\mathcal{B}}} \geq d_{\mathcal{B}}$ .

If  $\mathbf{u}_2 \neq \mathbf{0}$  then we distinguish two cases. If  $\mathbf{u}_4 = \mathbf{0}$  then

$$\begin{aligned} w_L(\mathbf{u}) &= w_L(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2|\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3|\mathbf{u}_1 + 3\mathbf{u}_2 + \mathbf{u}_3) \\ &= (w_L(\mathbf{u}_1) + w_L(\mathbf{u}_1 + \mathbf{u}_2)) + (w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3 + \mathbf{u}_2)) \\ &= (w_L(\mathbf{u}_1) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3)) + (w_L(\mathbf{u}_1 + \mathbf{u}_2)) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3 + \mathbf{u}_2) \\ &\geq w_L(2\mathbf{u}_2 + \mathbf{u}_3) + w_L(2\mathbf{u}_2 + \mathbf{u}_3) \text{ (by the triangle inequality)} \\ &\geq 2w_L(2\mathbf{u}_2 + \mathbf{u}_3). \end{aligned}$$

Note that  $2\mathbf{u}_2 \in \mathcal{B}$  and  $\mathbf{u}_3 \in \hat{\mathcal{B}} \subset \mathcal{B}$ . If  $\mathbf{u}_3 \neq 2\mathbf{u}_2$  then  $w_L(2\mathbf{u}_2 + \mathbf{u}_3) \geq d_{\mathcal{B}}$  and  $w_L(\mathbf{u}) \geq 2d_{\mathcal{B}}$ . If  $2\mathbf{u}_2 = \mathbf{u}_3$  then  $\mathbf{u}_2 \in \hat{\mathcal{B}}$  and  $w_L(\mathbf{u}_2) \geq d_{\mathcal{B}}$ . So,  $w_L(\mathbf{u}) = w_L(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2|\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2) \geq 2w_L(\mathbf{u}_2) \geq 2d_{\mathcal{B}}$ .

Using twice the triangle inequality, the case  $\mathbf{u}_4 \neq \mathbf{0}$  easily gives

$$\begin{aligned} w_L(\mathbf{u}) &= w_L(\mathbf{u}_1|\mathbf{u}_1 + \mathbf{u}_2) + w_L(\mathbf{u}_1 + 2\mathbf{u}_2 + \mathbf{u}_3|\mathbf{u}_1 + 3\mathbf{u}_2 + \mathbf{u}_3 + \mathbf{u}_4) \\ &\geq w_L(\mathbf{u}_2) + w_L(\mathbf{u}_2 + \mathbf{u}_4) \geq w_L(\mathbf{u}_4). \end{aligned}$$

Hence,  $d \geq \min\{4d_{\mathcal{A}}, 2d_{\mathcal{B}}, d_{\mathcal{C}}\}$ . But the equality holds after the following considerations.

Taking the specific vector  $\mathbf{u}_1 \in \mathcal{A}$  with minimum weight  $d_{\mathcal{A}}$  we obtain  $w_L(\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1) = 4d_{\mathcal{A}}$ .

Taking the specific vector  $\mathbf{u}_4 \in \mathcal{C}$  with minimum weight  $d_{\mathcal{C}}$  we obtain  $w_L(\mathbf{0}|\mathbf{0}|\mathbf{0}|\mathbf{u}_4) = d_{\mathcal{C}}$ .

Taking the specific vector  $\mathbf{u}_2 \in \mathcal{B}$  with minimum weight  $d_{\mathcal{B}}$  we obtain the following. Note that  $\mathcal{B} \subset \mathcal{B}'$  and so we can write the vector  $\mathbf{u}_2$  as  $\mathbf{u}_2 = \hat{\mathbf{v}} + 2\mathbf{w}'$ , where  $\hat{\mathbf{v}} \in \hat{\mathcal{B}}$  and  $\mathbf{w}' \in \mathcal{B}' \setminus \hat{\mathcal{B}}$ . Take the vector  $\mathbf{u}_2 = \hat{\mathbf{v}} + 2\mathbf{w}' \in \mathcal{B}'$  and, moreover, the vector  $\hat{\mathbf{u}} = 2\hat{\mathbf{v}} \in \hat{\mathcal{B}}$  and compose the vector  $(\mathbf{0}|\mathbf{u}_2|2\mathbf{u}_2 + \hat{\mathbf{u}}|3\mathbf{u}_2 + \hat{\mathbf{u}}) = (\mathbf{0}|\mathbf{u}_2|\mathbf{0}|\mathbf{u}_2)$  which belongs to  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$ . This vector has minimum Lee weight  $2d_{\mathcal{B}}$ .  $\square$

### 3 Quaternary Reed-Muller codes

The usual binary linear *RM* family of codes is one of the oldest and interesting family of codes. The codes in this family are easy to decode and their combinatorial properties are of great interest to produce new optimal codes.



For any integer  $m \geq 1$  the family of binary linear  $RM$  codes is given by the sequence  $RM(r, m)$ , where  $0 \leq r \leq m$ . The code  $RM(r, m)$  is called the  $r$ -th order binary linear Reed-Muller code of length  $n = 2^m$  and it is true that

$$RM(0, m) \subset RM(1, m) \subset \dots \subset RM(r-2, m) \subset RM(r-1, m) \subset RM(r, m).$$

Let  $0 \leq r \leq m$ ,  $m \geq 1$ . Following [12] the  $RM(r, m)$  code of order  $r$  can be constructed by using the Plotkin construction in the following way:

$$\begin{aligned} RM(0, m) &= \{\mathbf{0}, \mathbf{1}\}, \quad RM(m, m) = \mathbb{Z}_2^{2^m}, \\ RM(r, m) &= \{(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2) : \mathbf{u}_1 \in RM(r, m-1), \mathbf{u}_2 \in RM(r-1, m-1)\} \end{aligned}$$

It is important to note that if we fix  $m$ , once we know the sequence  $RM(r, m)$  for all  $0 \leq r \leq m$ , then it is easy to obtain the new sequence  $RM(r, m+1)$  by using the Plotkin construction (3).

Moreover, the codes in the  $RM$  family fulfill the basic properties summarized in the following theorem:

**Theorem 9 ([12])** *The binary linear Reed-Muller family of codes  $\{RM(r, m)\}$ ,  $0 \leq r \leq m$ , has the following properties:*

1. the length  $n = 2^m$ ,  $m \geq 1$ ;
2. the minimum distance  $d = 2^{m-r}$ ;
3. the dimension  $k = \sum_{i=0}^r \binom{m}{i}$ ;
4. the code  $RM(r-1, m)$  is a subcode of  $RM(r, m)$ ,  $r > 0$ . The code  $RM(0, m)$  is the repetition code with only one nonzero codeword (the all ones vector). The code  $RM(m, m)$  is the whole space  $\mathbb{Z}_2^{2^m}$  and  $RM(m-1, m)$  is the even code (that is, the code with all the vectors of even weight from  $\mathbb{Z}_2^{2^m}$ );
5. the code  $RM(1, m)$  is the binary linear Hadamard code and  $RM(m-2, m)$  is the extended binary Hamming code of parameters  $(2^m, 2^m - m - 1, 4)$ ;
6. the code  $RM(r, m)$  is the dual code of  $RM(m-1-r, m)$  for  $0 \leq r < m$ .

In the recent literature [7, 20, 2, 3] several families of quaternary linear codes have been proposed and studied trying to generalize the  $RM$  codes. However, when we take the corresponding  $\mathbb{Z}_4$ -linear codes, they do not satisfy all the properties in Theorem 9. This last requirement is the main goal of the present work, to construct new families of quaternary linear codes such that, after the Gray map, we obtain  $\mathbb{Z}_4$ -linear codes with the parameters and properties quoted in Theorem 9. The result of the present paper generalizes the results in [19].

Further we will refer to these quaternary linear Reed-Muller codes as  $\mathcal{RM}$  to distinguish them from the binary linear Reed-Muller codes  $RM$ . Contrary to the binary linear case, where there is only one  $RM$  family, in the quaternary case we have  $\lfloor \frac{m+1}{2} \rfloor$  families for each value of  $m$ . We will distinguish these families by using subindexes  $s$  from the set  $\{0, \dots, \lfloor \frac{m-1}{2} \rfloor\}$ .

Table 1:  $\mathcal{RM}(r, m)$  codes for  $m = 1$

		$(r, m)$	
		$(0, 1)$	$(1, 1)$
$N$		$(\gamma, \delta)$	
1	$(1, 0)$	$(0, 1)$	$\mathcal{RM}_0(r, 1)$

### 3.1 The family of $\mathcal{RM}(r, 1)$ codes

We begin by considering the trivial case of  $m = 1$ , that is, the case of codes of binary length  $n = 2^1$ . The quaternary linear Reed-Muller code  $\mathcal{RM}(0, 1)$  is the repetition code with only one nonzero codeword (the vector with only one quaternary coordinate of value 2). This quaternary linear code is of type  $(1; 1, 0)$ . The code  $\mathcal{RM}(1, 1)$  is the whole space  $\mathbb{Z}_4^1$ , so a quaternary linear code of type  $(1; 0, 1)$ .

These two codes,  $\mathcal{RM}(0, 1)$  and  $\mathcal{RM}(1, 1)$ , after the Gray map, give binary codes with the same parameters of the corresponding binary codes  $RM(r, 1)$  and with the same properties described in Theorem 9. In this case, when  $m = 1$ , not only these codes have the same parameters, but they have the same codewords.

We will refer to these codes as  $\mathcal{RM}_0(0, 1)$  and  $\mathcal{RM}_0(1, 1)$ , respectively, as it is shown in Table 1. In each entry of this table there are the parameters  $(\gamma, \delta)$  of the corresponding code of type  $(N; \gamma, \delta)$ .

Since we will need an specific representation for these codes in Table 1, we will agree in using further the following matrices as the generator matrices for each one of them. The generator matrix of  $\mathcal{RM}_0(0, 1)$  is  $\mathcal{G}_0(0, 1) = \begin{pmatrix} 2 \end{pmatrix}$  and the generator matrix of  $\mathcal{RM}_0(1, 1)$  is  $\mathcal{G}_0(1, 1) = \begin{pmatrix} 1 \end{pmatrix}$ .

### 3.2 Plotkin and BQ-Plotkin constructions

The first important point is to apply the Plotkin construction to quaternary linear Reed-Muller codes.

Let  $\mathcal{RM}_s(r, m-1)$  and  $\mathcal{RM}_s(r-1, m-1)$ ,  $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$ , be any two  $\mathcal{RM}$  codes of type  $(N; \gamma_{r, m-1}^s, \delta_{r, m-1}^s)$  and  $(N; \gamma_{r-1, m-1}^s, \delta_{r-1, m-1}^s)$ ; binary length  $n = 2^{m-1}$ ; number of codewords  $2^{k_r}$  and  $2^{k_{r-1}}$ ; minimum distance  $2^{m-r-1}$  and  $2^{m-r}$  respectively, where

$$k_r = \sum_{i=0}^r \binom{m-1}{i}, \quad k_{r-1} = \sum_{i=0}^{r-1} \binom{m-1}{i}.$$

**Theorem 10** *For any  $r$  and  $m \geq 2$ ,  $0 < r < m$ , the code obtained by using the Plotkin construction*

$$\mathcal{RM}_s(r, m) = \{(\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2) : \mathbf{u}_1 \in \mathcal{RM}_s(r, m-1), \mathbf{u}_2 \in \mathcal{RM}_s(r-1, m-1)\},$$

Table 2:  $\mathcal{RM}(r, m)$  codes for  $m = 2$

$N$	$(r, m)$		
	$(0, 2)$	$(1, 2)$	$(2, 2)$
	$(\gamma, \delta)$		
2	$(1, 0)$	$(1, 1)$	$(0, 2)$

where  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ , is a quaternary linear code of type  $(2N; \gamma_{r,m}^s, \delta_{r,m}^s)$ , where  $\gamma_{r,m}^s = \gamma_{r,m-1}^s + \gamma_{r-1,m-1}^s$  and  $\delta_{r,m}^s = \delta_{r,m-1}^s + \delta_{r-1,m-1}^s$ ; the binary length is  $n = 2^m$ ; the number of codewords is  $2^k$ , where  $k = \sum_{i=0}^r \binom{m}{i}$ , the code distance is  $2^{m-r}$  and  $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$ .

For  $r = 0$ , the code  $\mathcal{RM}_s(0, m)$  is the repetition code with only one nonzero codeword (the all twos vector). For  $r = m$ , the code  $\mathcal{RM}_s(m, m)$  is the whole space  $\mathbb{Z}_4^{2^{m-1}}$ .

*Proof:* The type  $(2N; \gamma_{r,m}^s, \delta_{r,m}^s)$  of the code  $\mathcal{RM}_s(r, m)$ , its size and the minimum distance can be computed from Proposition 2. Since  $\mathcal{RM}_s(r-1, m-1) \subset \mathcal{RM}_s(r, m-1)$  and  $\mathcal{RM}_s(r-2, m-1) \subset \mathcal{RM}_s(r-1, m-1)$ , then taking into account the codes given in the previous section by induction we get  $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$ .  $\square$

For  $m = 2$ , taking the  $\mathcal{RM}_0(r, 1)$  codes in Table 1 and applying Theorem 10 we obtain the codes in Table 2. The generator matrices for these codes are the following

$$\mathcal{RM}_0(0, 2) : \begin{pmatrix} 2 & 2 \end{pmatrix}; \mathcal{RM}_0(1, 2) : \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}; \mathcal{RM}_0(2, 2) : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (4)$$

For  $m = 3$ , it is well known that there exist two  $\mathbb{Z}_4$ -linear Hadamard codes [10]. So, our goal is to construct two families of quaternary linear Reed-Muller codes as it is shown in Table 3. The codes in the first row of Table 3 can be obtained due to the Plotkin construction from the codes of Table 2. But, the codes in the second row can not be obtained by using only the Plotkin construction. It is in this case that we need to exploit the new BQ-Plotkin construction as we will see later in this section.

Constructions of additive codes with the parameters of the binary linear Reed-Muller codes by using only the Plotkin construction were initiated in [16, 19].

**Lemma 11** *Let  $\{A_i\}$ ,  $i = 1, 2, 3, 4$ , be a family of four quaternary linear codes of types  $(N; \gamma_i, \delta_i)$  with generator matrices  $G_i$ , respectively. Let  $A'_i$  and  $\hat{A}_i$  be*

Table 3:  $\mathcal{RM}(r, m)$  codes for  $m = 3$

$N$	$(r, m)$				
	$(0, 3)$	$(1, 3)$	$(2, 3)$	$(3, 3)$	
	$(\gamma, \delta)$				
4	$(1, 0)$	$(2, 1)$	$(1, 3)$	$(0, 4)$	$\mathcal{RM}_0(r, 3)$
4	$(1, 0)$	$(0, 2)$	$(1, 3)$	$(0, 4)$	$\mathcal{RM}_1(r, 3)$

the codes generated by  $\mathcal{G}'_i$  and  $\hat{\mathcal{G}}_i$ , respectively, such that for  $i = 1, 2, 3$  it is true that

- (i)  $\mathcal{A}_i \subset \mathcal{A}_{i+1}$ ;
- (ii)  $\hat{\mathcal{A}}_i \subset \hat{\mathcal{A}}_{i+1}$ ;
- (iii)  $\mathcal{A}'_i \subset \mathcal{A}'_{i+1}$ ;
- (iv)  $\mathcal{A}'_i \subset \mathcal{A}_{i+1}$ .

Then, the family  $\{\mathcal{PC}(\mathcal{A}_{i+1}, \mathcal{A}_i)\}$  of the three codes  $\mathcal{PC}(\mathcal{A}_2, \mathcal{A}_1)$ ,  $\mathcal{PC}(\mathcal{A}_3, \mathcal{A}_2)$  and  $\mathcal{PC}(\mathcal{A}_4, \mathcal{A}_3)$  satisfies (i), (ii), (iii) and (iv) for  $i = 1, 2$  and the family  $\{\mathcal{BQ}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)\}$  of the two codes  $\mathcal{BQ}(\mathcal{A}_3, \mathcal{A}_2, \mathcal{A}_1)$  and  $\mathcal{BQ}(\mathcal{A}_4, \mathcal{A}_3, \mathcal{A}_2)$  satisfies the properties (i), (ii), (iii) and (iv) for  $i = 1$ .

*Proof:* It is straightforward to see that the Plotkin construction fulfills the properties.

For the BQ-Plotkin construction the property (i) is clear from Definition 7.

Now, the generator matrix of  $\hat{\mathcal{BQ}}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  has the following form:

$$\begin{pmatrix} \hat{\mathcal{G}}_{i+2} & \hat{\mathcal{G}}_{i+2} & \hat{\mathcal{G}}_{i+2} & \hat{\mathcal{G}}_{i+2} \\ 0 & \mathcal{G}'_{i+1} & 2\mathcal{G}'_{i+1} & 3\mathcal{G}'_{i+1} \\ 0 & 0 & \hat{\mathcal{G}}_{i+1} & \hat{\mathcal{G}}_{i+1} \\ 0 & 0 & 0 & \hat{\mathcal{G}}_i \end{pmatrix}. \quad (5)$$

Using the properties (ii) and (iii) for the matrices  $\mathcal{G}_i$ ,  $\mathcal{G}_{i+1}$ ,  $\mathcal{G}_{i+2}$ , we get the property (ii) for  $\mathcal{BQ}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  and  $i = 1$ .

Since, the generator matrix of  $\mathcal{BQ}'(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  has the form

$$\begin{pmatrix} \mathcal{G}'_{i+2} & \mathcal{G}'_{i+2} & \mathcal{G}'_{i+2} & \mathcal{G}'_{i+2} \\ 0 & \mathcal{G}'_{i+1} & 2\mathcal{G}'_{i+1} & 3\mathcal{G}'_{i+1} \\ 0 & 0 & \hat{\mathcal{G}}_{i+1} & \hat{\mathcal{G}}_{i+1} \\ 0 & 0 & 0 & \mathcal{G}'_i \end{pmatrix}, \quad (6)$$

using the properties (ii) and (iii) for the matrices  $\mathcal{G}_i, \mathcal{G}_{i+1}, \mathcal{G}_{i+2}$  we obtain the property (iii) for  $\mathcal{BQ}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  and  $i = 1$ .

Finally, the generator matrix of  $\mathcal{BQ}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  has the form

$$\begin{pmatrix} \mathcal{G}_{i+2} & \mathcal{G}_{i+2} & \mathcal{G}_{i+2} & \mathcal{G}_{i+2} \\ 0 & \mathcal{G}'_{i+1} & 2\mathcal{G}'_{i+1} & 3\mathcal{G}'_{i+1} \\ 0 & 0 & \hat{\mathcal{G}}_{i+1} & \hat{\mathcal{G}}_{i+1} \\ 0 & 0 & 0 & \mathcal{G}_i \end{pmatrix}. \quad (7)$$

Using the properties (ii), (iii) and (iv) for the matrices  $\mathcal{G}_i, \mathcal{G}_{i+1}, \mathcal{G}_{i+2}$  we obtain the property (iv) for  $\mathcal{BQ}(\mathcal{A}_{i+2}, \mathcal{A}_{i+1}, \mathcal{A}_i)$  and  $i = 1$ .  $\square$

Let  $\mathcal{RM}_{s-1}(r, m-2)$ ,  $\mathcal{RM}_{s-1}(r-1, m-2)$  and  $\mathcal{RM}_{s-1}(r-2, m-2)$ ,  $0 < s \leq \lfloor \frac{m-3}{2} \rfloor$ ,  $m > 3$ , be any three  $\mathcal{RM}$  codes of type  $(N; \gamma_{r,m-2}^{s-1}, \delta_{r,m-2}^{s-1})$ ,  $(N; \gamma_{r-1,m-2}^{s-1}, \delta_{r-1,m-2}^{s-1})$  and  $(N; \gamma_{r-2,m-2}^{s-1}, \delta_{r-2,m-2}^{s-1})$ ; binary length  $n = 2^{m-2}$ ; number of codewords  $2^{k_r}$ ,  $2^{k_{r-1}}$  and  $2^{k_{r-2}}$ ; minimum distances  $2^{m-r-2}$ ,  $2^{m-r-1}$  and  $2^{m-r}$  respectively, where

$$k_r = \sum_{i=0}^r \binom{m-2}{i}, \quad k_{r-1} = \sum_{i=0}^{r-1} \binom{m-2}{i}, \quad k_{r-2} = \sum_{i=0}^{r-2} \binom{m-2}{i}.$$

Let  $\mathcal{G}_s(r, m)$ ,  $0 < r < m-1$ , be the matrix

$$\begin{pmatrix} \mathcal{G}_{s-1}(r, m-2) & \mathcal{G}_{s-1}(r, m-2) & \mathcal{G}_{s-1}(r, m-2) & \mathcal{G}_{s-1}(r, m-2) \\ 0 & \mathcal{G}'_{s-1}(r-1, m-2) & 2\mathcal{G}'_{s-1}(r-1, m-2) & 3\mathcal{G}'_{s-1}(r-1, m-2) \\ 0 & 0 & \hat{\mathcal{G}}_{s-1}(r-1, m-2) & \hat{\mathcal{G}}_{s-1}(r-1, m-2) \\ 0 & 0 & 0 & \mathcal{G}_{s-1}(r-2, m-2) \end{pmatrix} \quad (8)$$

For the special case  $r = 1$  we need to define  $\mathcal{G}_{s-1}(-1, m-2)$  as the generator matrix of the all zero codeword code.

**Theorem 12** *For any  $r$  and  $m \geq 3$ ,  $0 < r < m-1$ , the  $\mathcal{RM}_s(r, m)$  code,  $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$ , obtained by using the BQ-Plotkin construction in Definition 7 and with the generator matrix  $\mathcal{G}_s(r, m)$  defined in (8), is a quaternary linear code of type  $(4N; \gamma_{r,m}^s, \delta_{r,m}^s)$ , where  $\gamma_{r,m}^s = \gamma_{r,m-2}^{s-1} + \gamma_{r-2,m-2}^{s-1}$ ;  $\delta_{r,m}^s = \delta_{r,m-2}^{s-1} + \gamma_{r-1,m-2}^{s-1} + 2\delta_{r-1,m-2}^{s-1} + \delta_{r-2,m-2}^{s-1}$ ; the binary length is  $n = 2^m$ ; the number of codewords is  $2^k$ , where  $k = \sum_{i=0}^r \binom{m}{i}$ ; the minimum distance is  $2^{m-r}$  and  $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$ .*

*Proof:* The type  $(4N; \gamma_{r,m}^s, \delta_{r,m}^s)$  of the code  $\mathcal{RM}_s(r, m)$  and the minimum distance can be computed from Proposition 8.

To compute the size note that

$$\begin{aligned} 2^k = |\mathcal{RM}_s(r, m)| &= |\mathcal{RM}_{s-1}(r, m-2)| \times |\mathcal{RM}'_{s-1}(r-1, m-2)| \\ &\quad \times |\hat{\mathcal{M}}_{s-1}(r-1, m-2)| \times |\mathcal{RM}_{s-1}(r-2, m-2)|, \end{aligned}$$

where  $\mathcal{RM}'_{s-1}(r-1, m-2)$  and  $\hat{\mathcal{RM}}_{s-1}(r-1, m-2)$  are the quaternary linear codes generated by  $\mathcal{G}'_{s-1}(r-1, m-2)$  and  $\hat{\mathcal{G}}_{s-1}(r-1, m-2)$ , respectively. Hence,

$$|\mathcal{RM}'_{s-1}(r-1, m-2)| \times |\hat{\mathcal{RM}}_{s-1}(r-1, m-2)| = 2^{2\gamma_{r-1, m-2}^{s-1} + 4\delta_{r-1, m-2}^{s-1}} = 2^{2k_{r-1}}$$

So,  $k = k_r + 2k_{r-1} + k_{r-2}$ . Finally, we obtain

$$\begin{aligned} k &= \sum_{i=0}^r \binom{m-2}{i} + 2 \sum_{i=0}^{r-1} \binom{m-2}{i} + \sum_{i=0}^{r-2} \binom{m-2}{i} \\ &= \sum_{i=0}^r \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} = \sum_{i=0}^r \binom{m}{i}. \end{aligned}$$

To prove that  $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$  notice that from Lemma 11 and since the codes of Table 1 and Table 2 fulfill the four conditions of this lemma we can conclude by induction that the code generated by the matrix  $\mathcal{G}_s(r-1, m)$  is a subcode of the code generated by the matrix  $\mathcal{G}_s(r, m)$ .  $\square$

For every  $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$  the family of codes  $\mathcal{RM}_s(r, m)$  constructed using the above theorem is incomplete in the sense that the codes  $\mathcal{RM}_s(-1, m)$ ,  $\mathcal{RM}_s(0, m)$ ,  $\mathcal{RM}_s(m-1, m)$ ,  $\mathcal{RM}_s(m, m)$  do not come from the construction. To be coherent with all the notations, for  $r = -1$ , the code  $\mathcal{RM}_s(-1, m)$  is defined as the all zero codeword code. For  $r = 0$ , the code  $\mathcal{RM}_s(0, m)$  is defined as the repetition code with only one non zero codeword (the all twos quaternary vector). For  $r = m-1$  and  $r = m$ , the codes  $\mathcal{RM}_s(m-1, m)$  and  $\mathcal{RM}_s(m, m)$  are defined as the even weight code and the whole space  $\mathbb{Z}_4^{2^{m-1}}$ , respectively. The construction of the families of Reed-Muller codes in Theorem 12 is based on the generator matrices and so, for each index  $s$ , we need a generator matrix for the codes  $\mathcal{RM}_s(-1, m)$ ,  $\mathcal{RM}_s(0, m)$ ,  $\mathcal{RM}_s(m-1, m)$ ,  $\mathcal{RM}_s(m, m)$ .

We will use the following generator matrices:  $\mathcal{G}_s(-1, m) = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}$ ,  $\mathcal{G}_s(0, m) = \begin{pmatrix} 2 & \cdots & 2 \end{pmatrix}$ ,  $\mathcal{G}_s(m, m) = I_{2^{m-1}}$ .

The generator matrix  $\mathcal{G}_s(m-1, m)$  will be recursively obtained by using the BQ-Plotkin construction  $\mathcal{BQ}(\mathcal{RM}_{s-1}(m-2, m-2), \mathcal{RM}_{s-1}(m-2, m-2), \mathcal{RM}_{s-1}(m-3, m-2))$  (see Definition 7).

**Proposition 13** *For  $m \geq 3$ , the matrix  $\mathcal{G}_s(m-1, m)$  of Definition 7 associated to  $\mathcal{BQ}(\mathcal{RM}_{s-1}(m-2, m-2), \mathcal{RM}_{s-1}(m-2, m-2), \mathcal{RM}_{s-1}(m-3, m-2))$  is a generator matrix of  $\mathcal{RM}_s(m-1, m)$ .*

*Proof:* All the rows in matrix  $\mathcal{G}_s(m-1, m)$  are vectors of even weight. So, to prove that this matrix generates  $\mathcal{RM}_s(m-1, m)$  we only need to check if the dimension is the adequate.

We will prove, by induction on  $m \geq 1$ , that  $\gamma_{m-1, m}^s = 1$  and  $\delta_{m-1, m}^s = 2^{m-1} - 1$ . The claim is trivially true for  $m = 1$  and  $m = 2$  using the matrices defined in section 3.1 and in (4). Suppose the claim is true for  $m \geq 2$ .

Table 4:  $\mathcal{RM}(r, m)$  codes for  $m = 4$

$N$	$(r, m)$					
	$(0, 4)$	$(1, 4)$	$(2, 4)$	$(3, 4)$	$(4, 4)$	
	$(\gamma, \delta)$					
8	$(1, 0)$	$(3, 1)$	$(3, 4)$	$(1, 7)$	$(0, 8)$	$\mathcal{RM}_0(r, 4)$
8	$(1, 0)$	$(1, 2)$	$(1, 5)$	$(1, 7)$	$(0, 8)$	$\mathcal{RM}_1(r, 4)$

Since the matrix  $\mathcal{G}_s(m-1, m)$  is upper triangular, we must to add the respective values  $\gamma$  and  $\delta$  of  $\mathcal{G}_{s-1}(m-2, m-2)$ ,  $\mathcal{G}'_{s-1}(m-2, m-2)$ ,  $\hat{\mathcal{G}}_{s-1}(m-2, m-2)$  and  $\mathcal{G}_{s-1}(m-3, m-2)$ .

By induction,  $\gamma_{m-3, m-2}^{s-1} = 1$  and  $\delta_{m-3, m-2}^{s-1} = 2^{m-3} - 1$ . Since  $\mathcal{G}'_{s-1}(m-2, m-2) = \hat{\mathcal{G}}_{s-1}(m-2, m-2) = \mathcal{G}_{s-1}(m-2, m-2)$  we have  $\gamma_{m-2, m-2}^{s-1} = 0$  and  $\delta_{m-2, m-2}^{s-1} = 2^{m-3}$ .

Hence, we obtain  $\gamma_{m-1, m}^s = 0 + 0 + 0 + 1 = 1$ ,  $\delta_{m-1, m}^s = 2^{m-3} + 2^{m-3} + 2^{m-3} + 2^{m-3} - 1 = 2^{m-1} - 1$ .  $\square$

Note that with these definitions of  $\mathcal{RM}_s(-1, m)$ ,  $\mathcal{RM}_s(0, m)$ ,  $\mathcal{RM}_s(m-1, m)$ ,  $\mathcal{RM}_s(m, m)$ , the family of codes  $\mathcal{RM}_s(r, m)$ ,  $0 \leq r \leq m$ ,  $0 < s \leq \lfloor \frac{m-1}{2} \rfloor$ , fulfills the four conditions of Lemma 11.

Using Theorems 10 and 12 we can construct the  $\mathcal{RM}$  codes in the two rows of Table 3. We do not write the generator matrices for codes  $\mathcal{RM}_0(r, 3)$  because they can be directly obtained from the respective codes for  $m = 2$  by using the Plotkin construction. For the codes in the family  $\mathcal{RM}_1(r, 3)$  we present the generator matrices as a direct application of Theorem 12:

$$\mathcal{RM}_1(0, 3) : \left( \begin{array}{cccc} 2 & 2 & 2 & 2 \end{array} \right); \mathcal{RM}_1(1, 3) : \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{array} \right); \mathcal{RM}_1(2, 3) : \left( \begin{array}{cccc} 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \end{array} \right) \quad (9)$$

and the remaining code  $\mathcal{RM}_1(3, 3)$  in the family is the whole space  $\mathbb{Z}_4^2$ .

All these codes, after the Gray map, give binary codes with the same parameters as the codes  $\mathcal{RM}(r, 3)$  and with the same properties described in Theorem 9. In the case  $m = 3$ , like in the case  $m = 2$  not only these codes have the same parameters, but they have the same codewords. This is not in this way for all the other values  $m > 3$ .

Now, from Table 3 and by using the Plotkin construction we can construct the two families of the codes  $\mathcal{RM}_s(r, 4)$  for  $s = 0, 1$ , as it is shown in Table 4. Note that the family of codes  $\mathcal{RM}_1(r, 4)$  also can be obtained using the BQ-Plotkin construction from the family of codes  $\mathcal{RM}_0(r, 2)$  in Table 2.

From the codes in Table 4 applying the Plotkin construction we can construct the two families of  $\mathcal{RM}_s(r, 5)$ ,  $s = 0, 1$ , as it is shown in Table 5. The third

Table 5:  $\mathcal{RM}(r, m)$  codes for  $m = 5$

$N$	$(r, m)$						
	$(0, 5)$	$(1, 5)$	$(2, 5)$	$(3, 5)$	$(4, 5)$	$(5, 5)$	
	$(\gamma, \delta)$						
16	$(1, 0)$	$(4, 1)$	$(6, 5)$	$(4, 11)$	$(1, 15)$	$(0, 16)$	$\mathcal{RM}_0(r, 5)$
16	$(1, 0)$	$(2, 2)$	$(2, 7)$	$(2, 12)$	$(1, 15)$	$(0, 16)$	$\mathcal{RM}_1(r, 5)$
16	$(1, 0)$	$(0, 3)$	$(2, 7)$	$(0, 13)$	$(1, 15)$	$(0, 16)$	$\mathcal{RM}_2(r, 5)$

family in Table 5,  $\mathcal{RM}_2(r, 5)$ , is obtained applying the BQ-Plotkin construction to the  $\mathcal{RM}_1(r, 3)$  family of Table 3.

Note that  $\mathcal{RM}_0(r, 5)$  only can be obtained applying the Plotkin construction,  $\mathcal{RM}_2(r, 5)$  only can be obtained applying the BQ-Plotkin construction, but  $\mathcal{RM}_1(r, 5)$  can be obtained by using the Plotkin or the BQ-Plotkin construction.

In general, for  $m > 1$ , the code  $\mathcal{RM}_0(r, m)$  can be only obtained applying the Plotkin construction. For  $m$  even and  $m$  odd, but  $s \neq \frac{m-1}{2}$ , families of  $\mathcal{RM}_s(r, m)$  can be obtained applying the Plotkin or the BQ-Plotkin construction. For  $m$  odd and  $s = \frac{m-1}{2}$ ,  $\mathcal{RM}_s(r, m)$  only can be obtained applying the BQ-Plotkin construction. A question arises at this point, how many families of Reed-Muller codes can be obtained combining the Plotkin and the BQ-Plotkin constructions? Next proposition proves that no new codes appear when we combine both these constructions.

Given three quaternary linear codes  $\mathcal{A}$ ,  $\mathcal{B}$  and  $\mathcal{C}$ , we remind that  $\mathcal{PC}(\mathcal{A}, \mathcal{B})$  is the quaternary linear code obtained applying the Plotkin construction (see Definition 1) and  $\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})$  is the quaternary linear code obtained by using the BQ-Plotkin construction (see Definition 7). The following proposition shows that the two constructions commute.

**Proposition 14** *Given four quaternary linear codes  $\mathcal{A}$ ,  $\mathcal{B}$ ,  $\mathcal{C}$  and  $\mathcal{D}$ , then the codes  $\mathcal{PC}(\mathcal{BQ}(\mathcal{A}, \mathcal{B}, \mathcal{C})), \mathcal{BQ}(\mathcal{B}, \mathcal{C}, \mathcal{D}))$  and  $\mathcal{BQ}(\mathcal{PC}(\mathcal{A}, \mathcal{B}), \mathcal{PC}(\mathcal{B}, \mathcal{C}), \mathcal{PC}(\mathcal{C}, \mathcal{D}))$  are permutationally equivalent.*

The proof is straightforward.

Notice that the same result is true changing the BQ-Plotkin construction by the quaternary Plotkin construction or the double Plotkin construction.

From now on, when we talk about the family of Reed-Muller codes  $\{\mathcal{RM}_s(r, m)\}$  constructed by using the Plotkin and the BQ-Plotkin constructions we will assume that for  $m$  even and  $m$  odd, but  $s \neq \frac{m-1}{2}$ , these families of codes are obtained applying the Plotkin construction. For  $m$  odd and  $s = \frac{m-1}{2}$ , the family of codes is obtained applying the BQ-Plotkin construction.

The following lemma computes the values for the parameters  $\gamma$  and  $\delta$  of the  $\mathcal{RM}_s(r, m)$  codes in the specific case when  $m$  is odd,  $m \geq 3$  and  $s = \frac{m-1}{2}$ .



**Lemma 15** For odd  $m$ ,  $m \geq 3$  and  $s = \frac{m-1}{2}$  we have the following values for the parameters  $\gamma_{r,m}^s$  and  $\delta_{r,m}^s$  of the  $\mathcal{RM}_s(r, m)$  code built by using the BQ-Plotkin construction with the generator matrix (8):

- (i) For odd  $r$  it is true that  $\gamma_{r,m}^s = 0$ .
- (ii) For even  $r$  we have  $\gamma_{r,m}^s = \binom{(m-1)/2}{r/2}$ .
- (iii) The following equalities  $\delta_{m,m}^s = 2^{m-1}$ ,  $\delta_{m-1,m}^s = 2^{m-1} - 1$  and  $\delta_{m-2,m}^s = 2^{m-1} - \frac{m+1}{2}$  are true.

*Proof:* Note that by Proposition 8 it is true that  $\gamma_{r,m}^s = \gamma_{r,m-2}^{s-1} + \gamma_{r-2,m-2}^{s-1}$  with  $\gamma_{0,1}^0 = 1$  and  $\gamma_{1,1}^0 = 0$ . Using induction we can prove (i) and (ii).

Clearly,  $\delta_{m,m}^s = 2^{m-1}$ ,  $\delta_{m-1,m}^s = 2^{m-1} - 1$ . The value of  $m$  is odd, hence  $m-2$  is also odd and  $\gamma_{m-2,m}^s = 0$ . So,  $|\mathcal{RM}_s(m-2, m)| = 2^{2\delta_{m-2,m}^s}$  but, also,  $|\mathcal{RM}_s(m-2, m)| = 2^{2^m - \binom{m-1}{2} - \binom{m}{2}}$ . Finally,  $2\delta_{m-2,m}^s = 2^m - m - 1$  and  $\delta_{m-2,m}^s = 2^{m-1} - \frac{m+1}{2}$ .  $\square$

As it is proved in Theorems 10 and 12 the constructed families of  $\mathcal{RM}$  codes satisfy the same properties we stated for binary linear Reed-Muller codes in Theorem 9 except for the duality. In the following Section we will discuss this topic.

Notice that, after the Gray map, the constructed  $\mathcal{RM}$  families of quaternary linear Reed-Muller codes have not only the same parameters as the usual binary linear family of  $RM$  codes, but also the characteristic properties of codes  $\mathcal{RM}_s(1, m)$  and  $\mathcal{RM}_s(m-2, m)$  as it is stated in the following proposition.

**Proposition 16** For any integer  $m \geq 1$  and  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ , after the Gray map the code  $\mathcal{RM}_s(1, m)$  is a  $\mathbb{Z}_4$ -linear Hadamard code and the code  $\mathcal{RM}_s(m-2, m)$  is an  $\mathbb{Z}_4$ -linear extended perfect code.

*Proof:* From Theorem 12 we have that the codes  $\mathcal{RM}_s(1, m)$ , where  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ , are quaternary linear and, under the Gray map, have the parameters of Hadamard codes. Analogously all the codes  $\mathcal{RM}_s(m-2, m)$ ,  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ , after the Gray map, are  $\mathbb{Z}_4$ -linear and have the parameters of extended perfect binary codes. By the Krotov classification [9, 10], these codes could be only  $\mathbb{Z}_4$ -linear Hadamard and extended  $\mathbb{Z}_4$ -linear perfect codes, respectively.  $\square$

## 4 Duality

For the usual binary linear  $RM$  codes we know that the codes  $RM(r, m)$  and  $RM(m-r-1, m)$  are dual to each other. The families of  $\mathcal{RM}$  codes have the same property if we use the Kronecker inner product to define the  $\mathbb{Z}_4$ -duality.

Throughout this section the notion of duality will be related to the Kronecker inner product defined in (2).

We begin by studying the duality properties for the family of  $\mathcal{RM}$  codes obtained by using the BQ-Plotkin construction, that is, we are going to prove the duality relationships for the family of codes  $\mathcal{RM}_s(r, m)$ ,  $m$  odd,  $s = \frac{m-1}{2}$ , constructed from the family  $\mathcal{RM}_{s-1}(r, m-2)$ .

Basically, we will prove this fact by induction but, previously, we need two technical lemmas. We will use  $\mathcal{G}_s(r, m)$  to refer to the generator matrix of code  $\mathcal{RM}_s(r, m)$ ; the matrices  $\mathcal{G}'_s(r, m)$ ,  $\hat{\mathcal{G}}_s(m-r-1, m)$  will have the meaning that we introduced in Definition 7 and  $\mathcal{RM}'_s(r, m)$ ,  $\hat{\mathcal{M}}_s(m-r-1, m)$  will be the codes generated by  $\mathcal{G}'_s(r, m)$  and  $\hat{\mathcal{G}}_s(m-r-1, m)$ , respectively.

**Lemma 17** *Let  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^N$  be any two vectors such that  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_2)$  and  $\mathbf{v} = (\mathbf{v}_1 | \mathbf{v}_2)$ , where  $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_4^{N/2}$ . Then,*

$$\langle (\mathbf{u}_1 | \mathbf{u}_2), (\mathbf{v}_1 | \mathbf{v}_2) \rangle_{\otimes N} = \langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_2, \mathbf{v}_2 \rangle_{\otimes N/2}. \quad (10)$$

*Proof:* Straightforward from the Kronecker inner product definition.  $\square$

**Lemma 18** *Let  $m$  be an odd integer,  $m \geq 3$ ,  $N = 2^{m-1}$  and  $s = \frac{m-1}{2}$ . Let  $\{\mathcal{RM}_s(r, m)\}$  be the family of  $\mathcal{RM}$  codes obtained in Theorem 12 by using the BQ-Plotkin construction. Then, for each  $0 \leq r \leq m$ , for all  $\mathbf{u} \in \mathcal{G}'_s(r, m) \setminus \hat{\mathcal{G}}_s(r, m)$  and  $\mathbf{v} \in \hat{\mathcal{M}}_s(m-r-1, m)$  we have  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0$ .*

*Proof:* We proceed by induction on  $m$  beginning with  $m = 3$ . Using (9) it is easy to see that the assertion is true for  $m = 3$ .

For the case when  $r$  is odd the statement is trivially true, since there is nothing to proof. Indeed, from Lemma 15,  $\gamma_{r,m}^s = 0$  and so  $\mathcal{G}'_s(r, m) \setminus \hat{\mathcal{G}}_s(r, m) = \emptyset$ . Hence, along this proof we can take  $r$  as an even integer.

Now, for  $m > 3$  and  $0 < r \leq m-2$ , assume by induction hypothesis that for all  $\mathbf{x} \in \mathcal{G}'_{s-1}(r, m-2) \setminus \hat{\mathcal{G}}_{s-1}(r, m-2)$  and  $\mathbf{y} \in \hat{\mathcal{M}}_{s-1}(m-r-3, m-2)$  is  $\langle \mathbf{x}, \mathbf{y} \rangle_{\otimes N/4} = 0$ .

Let  $\mathbf{v} \in \hat{\mathcal{M}}_s(m-r-1, m)$  and  $\mathbf{u} \in \mathcal{G}'_s(r, m) \setminus \hat{\mathcal{G}}_s(r, m)$ ,  $0 < r \leq m-2$ . We will prove by induction that  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0$ .

From Proposition 8, we have  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1 | \mathbf{u}_1) + (0 | 0 | 0 | \mathbf{u}_4)$ , where  $\mathbf{u}_1 \in \mathcal{G}'_{s-1}(r, m-2) \setminus \hat{\mathcal{G}}_{s-1}(r, m-2)$  and  $\mathbf{u}_4 \in \mathcal{G}'_{s-1}(r-2, m-2) \setminus \hat{\mathcal{G}}_{s-1}(r-2, m-2)$ .

Also, we have  $\mathbf{v} = (\mathbf{v}_1 | \mathbf{v}_1 | \mathbf{v}_1 | \mathbf{v}_1) + (0 | \mathbf{v}_2 | 2\mathbf{v}_2 | 3\mathbf{v}_2) + (0 | 0 | \mathbf{v}_3 | \mathbf{v}_3) + (0 | 0 | 0 | \mathbf{v}_4)$  with  $\mathbf{v}_1 \in \hat{\mathcal{M}}_{s-1}(m-r-1, m-2)$ ,  $\mathbf{v}_2 \in \mathcal{RM}'_{s-1}(m-r-2, m-2)$ ,  $\mathbf{v}_3 \in \mathcal{RM}_{s-1}(m-r-2, m-2)$  and  $\mathbf{v}_4 \in \hat{\mathcal{M}}_{s-1}(m-r-3, m-2)$ .

Now, by using Lemma 17:

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} &= 8\langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/4} + 12\langle \mathbf{u}_1, \mathbf{v}_2 \rangle_{\otimes N/4} + 4\langle \mathbf{u}_1, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} \\ &\quad + \langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4} + 3\langle \mathbf{u}_4, \mathbf{v}_2 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_4 \rangle_{\otimes N/4} \\ &= \langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{z} \rangle_{\otimes N/4}, \end{aligned}$$

where  $\mathbf{z} = 3\mathbf{v}_2 + \mathbf{v}_3 + \mathbf{v}_4$ .

By induction hypothesis  $\langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} = \langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4} = 0$  and so we need only to show that  $\langle \mathbf{u}_4, \mathbf{z} \rangle_{\otimes N/4} = 0$ .

From Lemma 11 we have  $\hat{\mathcal{RM}}_{s-1}(m-r-3, m-2) \subset \hat{\mathcal{RM}}_{s-1}(m-r-2, m-2) \subset \hat{\mathcal{RM}}_{s-1}(m-r-1, m-2)$  and so  $\mathbf{v}_3 + \mathbf{v}_4 \in \hat{\mathcal{RM}}_{s-1}(m-r-1, m-2)$ .

As we said at the beginning of the proof,  $r$  is even. Therefore, we have that  $m-r-2$  is odd and from Lemma 15, we obtain  $\gamma_{m-r-2, m-2}^{s-1} = 0$ . Hence,  $\mathcal{G}'_{s-1}(m-r-2, m-2) = \hat{\mathcal{G}}_{s-1}(m-r-2, m-2)$  and  $\mathbf{z} = 3\mathbf{v}_2 + \mathbf{v}_3 + \mathbf{v}_4 \in \hat{\mathcal{RM}}_{s-1}(m-r-1, m-2)$ . But  $\mathbf{u}_4 \in \mathcal{G}'_{s-1}(r-2, m-2) \setminus \hat{\mathcal{G}}_{s-1}(r-2, m-2)$ . Then, by induction hypothesis,  $\langle \mathbf{u}_4, \mathbf{z} \rangle_{\otimes N/4} = 0$ .

Finally, we prove the statement for  $r = 0$ ;  $r = m-1$  and  $r = m$ .

For  $r = 0$ , we proceed by induction. Case  $m = 3$  is trivially true taking into account (9). We have  $\mathbf{u} \in \mathcal{G}'_s(0, m) \setminus \hat{\mathcal{G}}_s(0, m)$  and so  $\mathbf{u}$  is the all ones vector  $\mathbf{u} = (1, 1, \dots, 1)$ . Any vector  $\mathbf{v} \in \hat{\mathcal{RM}}_s(m-1, m)$  is generated by the rows of  $\hat{\mathcal{G}}_s(m-1, m)$ , where  $\mathcal{G}_s(m-1, m)$  is the matrix defined in (8). Hence,  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = \langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} = 0$ , by induction hypothesis, since  $\mathbf{u}_1 \in \mathcal{G}'_{s-1}(0, m-2) \setminus \hat{\mathcal{G}}_{s-1}(0, m-2)$  and  $\mathbf{v}_4 \in \hat{\mathcal{RM}}_{s-1}(m-3, m-2)$ .

For  $r = m-1$  we have  $\mathbf{u} = (0, 0, \dots, 0, 1) \in \mathcal{G}'_s(m-1, m) \setminus \hat{\mathcal{G}}_s(m-1, m)$  and  $\mathbf{v} = (0, 0, \dots, 0) \in \hat{\mathcal{G}}_s(0, m)$ , therefore  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0$ .

Finally, for  $r = m$  the claim is trivially true, because the set  $\mathcal{G}'_s(m, m) \setminus \hat{\mathcal{G}}_s(m, m)$  is empty.

□

**Theorem 19** *Let  $m$  be an odd integer,  $m \geq 1$ ,  $N = 2^{m-1}$  and  $s = \frac{m-1}{2}$  the set  $\{\mathcal{RM}_s(r, m)\}$  be the family of  $\mathcal{RM}$  codes obtained in Theorem 12 by using the BQ-Plotkin construction. Then, for each  $0 \leq r \leq m$ , the code  $\mathcal{RM}_s(r, m)$  is a quaternary dual of the code  $\mathcal{RM}_s(m-r-1, m)$ .*

*Proof:* Since  $|\mathcal{RM}_s(r, m)| \cdot |\mathcal{RM}_s(m-r-1, m)| = 2^m$ , it suffices to prove that for every  $\mathbf{u} \in \mathcal{G}_s(r, m)$  and  $\mathbf{v} \in \mathcal{G}_s(m-r-1, m)$  we have  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0$ . We proceed by induction on  $m$ . The claim is trivially true for  $m = 1$ .

Now, for  $m > 1$  and  $0 \leq r \leq m$ , assume by induction hypothesis that for all  $\mathbf{x} \in \mathcal{G}_{s-1}(r, m-2)$  and  $\mathbf{y} \in \mathcal{G}_{s-1}(m-r-3, m-2)$  it is true that  $\langle \mathbf{x}, \mathbf{y} \rangle_{\otimes N/4} = 0$ .

Let  $\mathbf{u} \in \mathcal{G}_s(r, m)$  and  $\mathbf{v} \in \mathcal{G}_s(m-r-1, m)$  for any  $0 < r \leq m$ .

When  $0 < r \leq m-2$  we can use the following expressions for  $\mathbf{u}$  and  $\mathbf{v}$ :

$\mathbf{u} = (\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1|\mathbf{u}_1) + (\mathbf{0}|\mathbf{u}_2|2\mathbf{u}_2|3\mathbf{u}_2) + (\mathbf{0}|\mathbf{0}|\mathbf{u}_3|\mathbf{u}_3) + (\mathbf{0}|\mathbf{0}|\mathbf{0}|\mathbf{u}_4)$ , where  $\mathbf{u}_1 \in \mathcal{G}_{s-1}(r, m-2)$ ,  $\mathbf{u}_2 \in \mathcal{G}'_{s-1}(r-1, m-2)$ ,  $\mathbf{u}_3 \in \hat{\mathcal{G}}_{s-1}(r-1, m-2)$  and  $\mathbf{u}_4 \in \mathcal{G}_{s-1}(r-2, m-2)$ ;

$\mathbf{v} = (\mathbf{v}_1|\mathbf{v}_1|\mathbf{v}_1|\mathbf{v}_1) + (\mathbf{0}|\mathbf{v}_2|2\mathbf{v}_2|3\mathbf{v}_2) + (\mathbf{0}|\mathbf{0}|\mathbf{v}_3|\mathbf{v}_3) + (\mathbf{0}|\mathbf{0}|\mathbf{0}|\mathbf{v}_4)$ , where  $\mathbf{v}_1 \in \mathcal{G}_{s-1}(m-r-1, m-2)$ ,  $\mathbf{v}_2 \in \mathcal{G}'_{s-1}(m-r-2, m-2)$ ,  $\mathbf{v}_3 \in \hat{\mathcal{G}}_{s-1}(m-r-2, m-2)$  and  $\mathbf{v}_4 \in \mathcal{G}_{s-1}(m-r-3, m-2)$ .

Therefore, applying Lemma 17 we get

$$\begin{aligned}
\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} &= 8\langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/4} + 12\langle \mathbf{u}_1, \mathbf{v}_2 \rangle_{\otimes N/4} + 4\langle \mathbf{u}_1, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} + \\
&\quad 12\langle \mathbf{u}_2, \mathbf{v}_1 \rangle_{\otimes N/4} + 24\langle \mathbf{u}_2, \mathbf{v}_2 \rangle_{\otimes N/4} + 9\langle \mathbf{u}_2, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_2, \mathbf{v}_4 \rangle_{\otimes N/4} + \\
&\quad 4\langle \mathbf{u}_3, \mathbf{v}_1 \rangle_{\otimes N/4} + 9\langle \mathbf{u}_3, \mathbf{v}_2 \rangle_{\otimes N/4} + 4\langle \mathbf{u}_3, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_3, \mathbf{v}_4 \rangle_{\otimes N/4} + \\
&\quad \langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4} + 3\langle \mathbf{u}_4, \mathbf{v}_2 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_4 \rangle_{\otimes N/4} \\
&= \langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4} + \langle \mathbf{u}_2, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_2, \mathbf{v}_4 \rangle_{\otimes N/4} + \langle \mathbf{u}_3, \mathbf{v}_2 \rangle_{\otimes N/4} + \langle \mathbf{u}_3, \mathbf{v}_4 \rangle_{\otimes N/4} + \\
&\quad \langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4} + 3\langle \mathbf{u}_4, \mathbf{v}_2 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_3 \rangle_{\otimes N/4} + \langle \mathbf{u}_4, \mathbf{v}_4 \rangle_{\otimes N/4}.
\end{aligned} \tag{11}$$

All the terms in the above equation are zero as can be seen by induction hypothesis either directly for  $\langle \mathbf{u}_1, \mathbf{v}_4 \rangle_{\otimes N/4}$  and  $\langle \mathbf{u}_4, \mathbf{v}_1 \rangle_{\otimes N/4}$ ; or using Lemma 11 for  $\langle \mathbf{u}_2, \mathbf{v}_4 \rangle_{\otimes N/4}$  and  $\langle \mathbf{u}_4, \mathbf{v}_2 \rangle_{\otimes N/4}$ ; or by Lemma 18 for  $\langle \mathbf{u}_2, \mathbf{v}_3 \rangle_{\otimes N/4}$  and  $\langle \mathbf{u}_3, \mathbf{v}_2 \rangle_{\otimes N/4}$ ; or applying the inclusions  $\mathcal{RM}_{s-1}(m-r-3, m-2) \subset \mathcal{RM}_{s-1}(m-r-2, m-2) \subset \mathcal{RM}_{s-1}(m-r-1, m-2)$  (see Theorem 12) as in  $\langle \mathbf{u}_3, \mathbf{v}_4 \rangle_{\otimes N/4}$ ,  $\langle \mathbf{u}_4, \mathbf{v}_3 \rangle_{\otimes N/4}$  and  $\langle \mathbf{u}_4, \mathbf{v}_4 \rangle_{\otimes N/4}$ .

It remains to prove that the statement is true for two cases:  $\mathbf{u} \in \mathcal{G}_s(m-1, m)$ ,  $\mathbf{v} \in \mathcal{G}_s(0, m)$  and  $\mathbf{u} \in \mathcal{G}_s(m, m)$ ,  $\mathbf{v} \in \mathcal{G}_s(-1, m)$ .

In the first case  $\mathbf{v} = (2, 2, \dots, 2)$  and  $\mathcal{G}_s(m-1, m)$  is an even code. In the second case  $\mathbf{v} = (0, 0, \dots, 0)$ . Therefore, in both these cases the statement is also true.  $\square$

Now we are going to prove the duality relationship for the families of codes obtained by using the Plotkin construction.

**Theorem 20** *For any integer  $m \geq 2$ , let  $\{\mathcal{RM}_s(r, m)\}$  be any families of  $\mathcal{RM}$  codes obtained in Theorem 10 by using the Plotkin construction. Then, for each  $0 \leq r < m$ , the code  $\mathcal{RM}_s(r, m)$  is the quaternary dual of the code  $\mathcal{RM}_s(m-r-1, m)$ .*

*Proof:* Since  $|\mathcal{RM}_s(r, m)| \cdot |\mathcal{RM}_s(m-r-1, m)| = 2^m$ , it suffices to show that for any  $\mathbf{u} \in \mathcal{G}_s(r, m)$  and  $\mathbf{v} \in \mathcal{G}_s(m-r-1, m)$  we have  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = 0$ . We proceed by induction on  $m$ . The claim is trivially true for  $m = 2$ , see (4). For even  $m$  and any  $s \leq \lfloor \frac{m-1}{2} \rfloor$ , all the codes of the family  $\mathcal{RM}_s(r, m)$  are constructed by using the Plotkin construction from the family  $\mathcal{RM}_s(r, m-1)$ . The same happens when  $m$  is odd and  $s < \frac{m-1}{2}$ . But for  $m$  odd and  $s = \frac{m-1}{2}$  the codes of the family  $\mathcal{RM}_s(r, m)$  are constructed by using the BQ-Plotkin construction from  $\mathcal{RM}_{s-1}(r, m-2)$ . Hence, the initial case for the induction proof is not only  $m = 1$ , but any  $m$  odd and  $s = \frac{m-1}{2}$ . This specific case was proved in Theorem 19.

Now, suppose the claim is true for the family of codes  $\mathcal{RM}_s(r, m-1)$ ,  $0 \leq r < m-1$  and  $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$ . Let  $\mathbf{u} = (\mathbf{u}_1 | \mathbf{u}_1 + \mathbf{u}_2)$ , where  $\mathbf{u}_1 \in \mathcal{G}_s(r, m-1)$ ,  $\mathbf{u}_2 \in \mathcal{G}_s(r-1, m-1)$  and  $\mathbf{v} = (\mathbf{v}_1 | \mathbf{v}_1 + \mathbf{v}_2)$ , where  $\mathbf{v}_1 \in \mathcal{G}_s(m-r-1, m-1)$ ,  $\mathbf{v}_2 \in \mathcal{G}_s(m-r-2, m-1)$ .

From Lemma 17 we have:  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = \langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle (\mathbf{u}_1 + \mathbf{u}_2), (\mathbf{v}_1 + \mathbf{v}_2) \rangle_{\otimes N/2} = \langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_1, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_1, \mathbf{v}_2 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_2, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_2, \mathbf{v}_2 \rangle_{\otimes N/2} = 3\langle \mathbf{u}_1, \mathbf{v}_2 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_2, \mathbf{v}_1 \rangle_{\otimes N/2} + 3\langle \mathbf{u}_2, \mathbf{v}_2 \rangle_{\otimes N/2}$ .

By induction hypothesis,  $\langle \mathbf{u}_1, \mathbf{v}_2 \rangle_{\otimes N/2} = 0$  and  $\langle \mathbf{u}_2, \mathbf{v}_1 \rangle_{\otimes N/2} = 0$ . Moreover,  $\langle \mathbf{u}_2, \mathbf{v}_2 \rangle_{\otimes N/2} = 0$ , since  $\mathcal{RM}_s(r-1, m-1) \subset \mathcal{RM}_s(r, m-1)$ .  $\square$

We summarize the properties of the  $\mathcal{RM}$  codes in the following theorem:

**Theorem 21** *For  $m \geq 1$ , the quaternary linear Reed-Muller family of codes  $\{\mathcal{RM}_s(r, m)\}$ ,  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ ,  $0 \leq r \leq m$ , has the following properties:*

1. *the binary length equals  $n = 2^m$ ,  $m \geq 1$ ;*
2. *the minimum distance is  $d = 2^{m-r}$ ;*
3. *the number of codewords is  $2^k$ , where  $k = \sum_{i=0}^r \binom{m}{i}$ ;*
4. *each code  $\mathcal{RM}_s(r-1, m)$  is a subcode of the code  $\mathcal{RM}_s(r, m)$ ,  $r > 0$ . The code  $\mathcal{RM}_s(0, m)$  is the repetition code with only one nonzero codeword (the all twos vector). The code  $\mathcal{RM}_s(m, m)$  is the whole space  $\mathbb{Z}_4^{2^{m-1}}$  and  $\mathcal{RM}_s(m-1, m)$  is the even code (i.e. the code with all the vectors of even weight);*
5. *the codes  $\mathcal{RM}_s(1, m)$  and  $\mathcal{RM}_s(m-2, m)$ , under the Gray map, are a  $\mathbb{Z}_4$ -linear Hadamard and a  $\mathbb{Z}_4$ -linear extended perfect codes respectively;*
6. *the code  $\mathcal{RM}_s(r, m)$  is the dual code of the code  $\mathcal{RM}_s(m-1-r, m)$  for  $-1 \leq r \leq m$ .*

In this section we used everywhere the Kronecker inner product to define the duality relationship. But it is also possible to use the standard definition of inner product given in (1) and, in this case, instead of the property 6) into the above Theorem, we obtain an alternative property 6') that we state as a new result:

**Theorem 22** *For  $m \geq 1$  and  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$ , given a quaternary linear Reed-Muller family  $\{\mathcal{RM}_s(r, m)\}$  of codes,  $0 \leq r \leq m$ , there exists a family of quaternary linear Reed-Muller codes  $\{\overline{\mathcal{RM}}_s(r, m)\}$ , monomially equivalent to  $\{\mathcal{RM}_s(r, m)\}$ , such that the code  $\overline{\mathcal{RM}}_s(r, m)$  is the dual code (by the standard inner product) of  $\mathcal{RM}_s(m-1-r, m)$  for  $-1 \leq r \leq m$ .*

*Proof:* We have  $\langle \mathbf{u}, \mathbf{v} \rangle_{\otimes N} = \mathbf{u} \cdot K_N \cdot \mathbf{v}^t = \langle \mathbf{u}, \mathbf{v} \cdot K_N \rangle$ . Hence, we define the code  $\overline{\mathcal{RM}}_s(r, m)$  as the code generated by a matrix  $\overline{\mathcal{G}}_s(r, m)$ , where  $\overline{\mathcal{G}}_s(r, m) = \mathcal{G}_s(r, m) \cdot K_N$ . Note that the code generated by the matrix  $\overline{\mathcal{G}}_s(r, m)$  is monomially equivalent to the code generated by  $\mathcal{G}_s(r, m)$ .  $\square$

## 5 Conclusion

New constructions based on quaternary linear codes has been proposed such that, after doing a Gray map, the obtained  $\mathbb{Z}_4$ -linear codes fulfill the same properties and fundamental characteristics as the binary linear  $RM$  codes. Apart from the parameters characterizing each code an important property which remains in these new presented families is that the first order  $RM$  code is, under the Gray map, a  $\mathbb{Z}_4$ -linear Hadamard code and the  $(m-2)$ -th order  $RM$  code, after the Gray map, is a  $\mathbb{Z}_4$ -linear extended perfect code, like in the usual binary case. So the families of codes obtained in the paper, after the Gray map, contain the families of  $\mathbb{Z}_4$ -linear extended perfect and  $\mathbb{Z}_4$ -linear Hadamard codes introduced in [9, 10]. Moreover, it is important to note that, after defining the Kronecker inner product, the codes  $RM(r, m)$  and  $RM(m-r-1, m)$  are dual each other like in the binary linear case.

There are several questions and subjects related to this work where would be of great interest to go deeply. The first one is about the generalization of the constructions of  $RM$  codes to the case of general additive codes, so the case of additive codes with  $\alpha \neq 0$ . It is known from [5] that there exist  $\mathbb{Z}_2\mathbb{Z}_4$ -linear perfect and Hadamard codes (which are not  $\mathbb{Z}_4$ -linear) and these could be the starting point of the new families. Other questions of interest are related to uniqueness (up to equivalence) of the codes in a given family of  $RM$  codes, weight distribution, etc.

## References

- [1] A. Bonnetcaze, P. Solé, and A.R. Calderbank, “Quaternary quadratic residue codes and unimodular lattices,” *IEEE Trans. Inform. Theory*, V. 41. P. 366–377, 1995.
- [2] J. Borges, C. Fernández, and K. T. Phelps, “Quaternary Reed-Muller codes,” *IEEE Trans. Inform. Theory*, V. 51. N. 7. P. 2686–2691, 2005.
- [3] J. Borges, C. Fernández, and K. T. Phelps, “ZRM codes,” to appear in *IEEE Trans. Inform. Theory*, 2007.
- [4] J. Borges, C. Fernández, J. Pujol, J. Rifà, and M. Villanueva, “ $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality,” submitted to *IEEE Trans. Inform. Theory*, 2007. Preprint available at <http://arxiv.org/abs/0710.1149>.
- [5] J. Borges, and J. Rifà, “A characterization of 1-perfect additive codes,” *IEEE Trans. Inform. Theory*, V. 45. N. 5. P. 1688–1697, 1999.
- [6] P. Delsarte, “An algebraic approach to the association schemes of coding theory,” *Philips Research Rep. Suppl.*, V. 10, 1973.
- [7] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, “The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals and related codes,” *IEEE Trans. Inform. Theory*, V. 40. P. 301–319, 1994.

- [8] X-D. Hou, J.T. Lahtonen, and S. Koponen, "The Reed-Muller Code  $R(r, m)$  is not  $\mathbb{Z}_4$ -linear for  $3 \leq r \leq m - 2$ ," *IEEE Trans. Inform. Theory*, V. 44. P. 798–799, 1998.
- [9] D. S. Krotov, " $\mathbb{Z}_4$ -linear perfect codes," *Discrete analysis and operation research*, Novosibirsk, Institute of Math. SB RAS, V. 7. N. 4. P. 78-90, 2000. Translation available at <http://arxiv.org/abs/0710.0198>.
- [10] D. S. Krotov, " $\mathbb{Z}_4$ -linear Hadamard and extended perfect codes," in *International Workshop on Coding and Cryptography* Paris (France) P. 329-334, Jan. 8-12, 2001.
- [11] C. Y. Lee, "Some properties of nonbinary error-correcting codes," *IRE Trans. Inform. Theory*, V. 4. N. 4. P. 77–82, June 1958.
- [12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
- [13] A. A. Nechaev, "Kerdock codes in a cyclic form," *Disc. Math.* V. 1. N. 4. P. 123–139, 1989.
- [14] K. Phelps, J. Rifà and M. Villanueva, "On the Additive ( $\mathbb{Z}_4$ -Linear and Non- $\mathbb{Z}_4$ -Linear) Hadamard Codes: Rank and Kernel". *IEEE Trans. Inform. Theory*, vol. 52, n. 1, pp. 316-319, January 2006.
- [15] M. Plotkin, "Binary codes with specified minimum distances," *IEEE Trans. Inform. Theory*, V. 6. P. 445–450, 1960.
- [16] J. Pujol and J. Rifà, "Additive Reed-Muller codes," *Proc. of Int. Symp. on Inform. Theory*, Ulm, Germany, P. 508, 1997.
- [17] J. Pujol, J. Rifà and F. I. Solov'eva, "Quaternary Plotkin constructions and Quaternary Reed-Muller codes". *Lecture Notes in Computer Science*, 4851 P. 148–157, 2007.
- [18] J. Rifà and J. Pujol, "Translation invariant propelinear codes," *IEEE Trans. Inform. Theory*, V. 43. P. 590–598, 1997.
- [19] F. I. Solov'eva, "On  $\mathbb{Z}_4$ -linear codes with parameters of Reed-Muller codes," *Problems of Inform. Trans.* V. 43. N. 1. P. 26–32, 2007.
- [20] Zhe-Xian Wan, *Quaternary codes*, Singapore: World Scientific Publishing Co. Pte. Ltd, 1997.